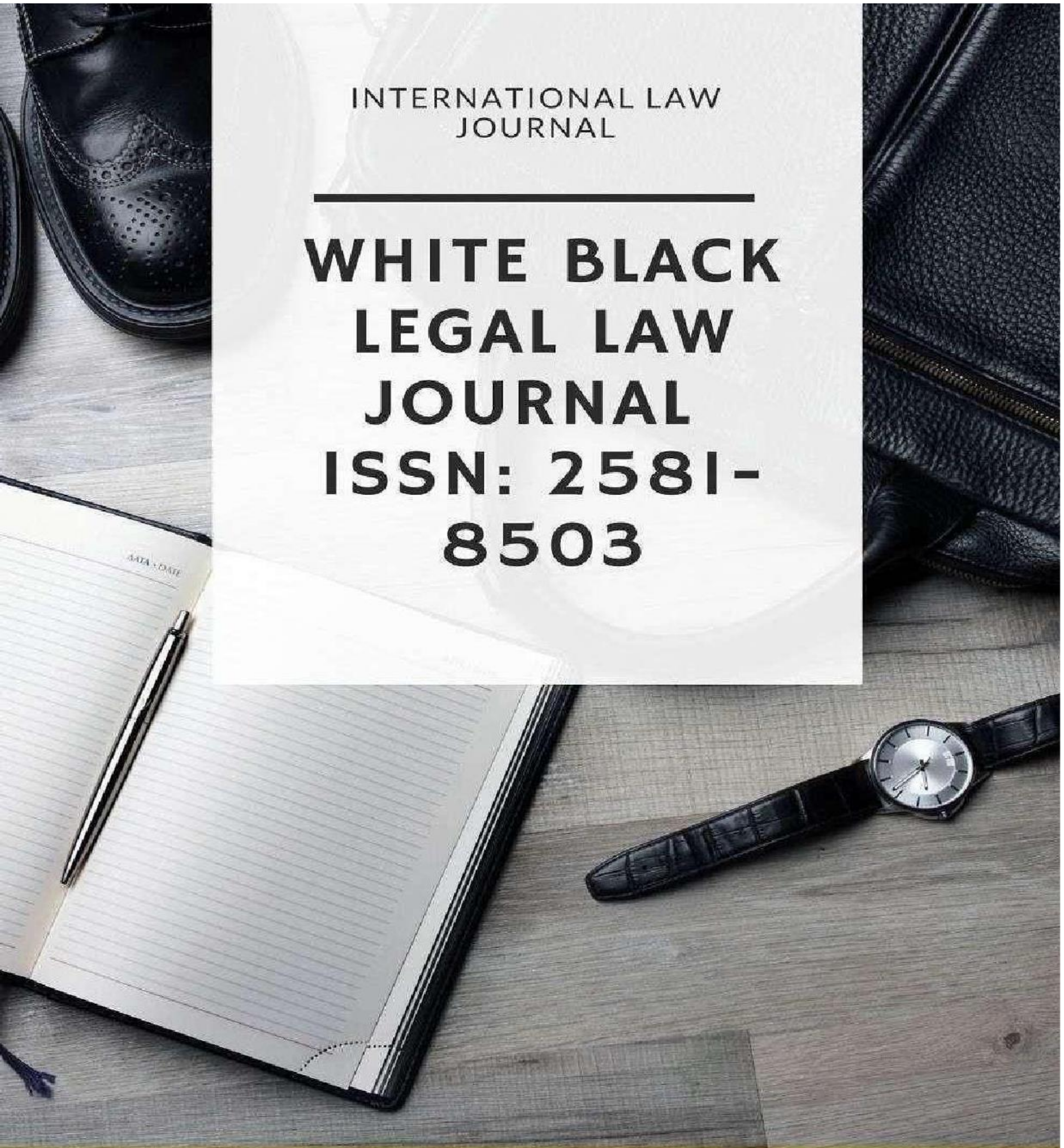

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

 ISSN: 2581-8503

THE ROLE OF ARTIFICIAL INTELLIGENCE IN ENHANCING CORPORATE GOVERNANCE AND BOARD ACCOUNTABILITY IN INDIA

AUTHORED BY - MONIKA GIRI
M.A. LL.M.

Abstract

Artificial Intelligence (AI) is increasingly transforming corporate governance by enabling companies to improve decision-making, risk management, compliance, transparency and accountability. In India, the growing adoption of AI by corporations has created new opportunities for boards of directors to analyse large volumes of financial, operational and regulatory data and identify potential risks at an early stage. AI-based systems can assist boards in monitoring corporate performance, detecting irregular transactions, identifying cybersecurity threats and strengthening internal control mechanisms. Such applications can contribute to more informed and evidence-based decision-making while reducing delays associated with conventional governance processes.

The integration of AI, however, also raises significant questions concerning board accountability**.** Under the Companies Act, 2013, directors continue to bear statutory and fiduciary responsibilities even when corporate decisions are supported by automated or algorithmic systems. Reliance on AI cannot completely transfer responsibility from human decision-makers to technology. Boards must therefore establish appropriate mechanisms for algorithmic oversight, transparency, explainability, data governance and continuous monitoring of AI systems. Particular attention is required where AI-generated recommendations influence financial reporting, risk assessment, corporate disclosures or strategic decisions.

Furthermore, AI-driven governance must be harmonised with India's emerging digital regulatory framework, including data protection, cybersecurity and information technology requirements. Effective corporate governance therefore requires boards to understand both the opportunities and risks associated with AI. The study examines how AI can strengthen corporate governance and board accountability in India while addressing issues of liability, transparency, ethical decision-making, cybersecurity and regulatory compliance. It seeks to assess whether the existing Indian legal framework is sufficiently equipped to regulate AI-assisted corporate governance and proposes measures for developing responsible, transparent and accountable AI governance practices.

Keywords: Artificial Intelligence; Corporate Governance; Board Accountability; Directors' Duties; Regulatory Compliance.

Introduction

Artificial Intelligence ('AI') has emerged as a transformative technology capable of reshaping the manner in which corporations make decisions, manage risks, undertake compliance and exercise board-level oversight. Traditionally, corporate governance has been founded upon principles of transparency, accountability, fiduciary responsibility, disclosure, stakeholder protection and responsible decision-making by human directors. The increasing deployment of AI in areas such as financial analysis, fraud detection, risk assessment, regulatory compliance, cybersecurity, auditing and strategic forecasting, however, introduces a new technological dimension to these traditional principles. AI systems can process substantial quantities of corporate information and identify patterns, anomalies and potential risks more rapidly than conventional human-led processes. Consequently, AI may become an important instrument for boards of directors seeking to improve the quality and timeliness of corporate decision-making. The legal foundation for board accountability in India is principally contained in the Companies Act, 2013. Section 166 expressly establishes the statutory duties of directors. Under section 166(2), a director is required to act in good faith in order to promote the objects of the company for the benefit of its members as a whole and in the best interests of the company, its employees, shareholders, community and for the protection of the environment.1 The provision is particularly significant in the context of AI because the delegation of analytical or decision-support functions to an algorithm does not eliminate the statutory responsibility of the director. AI may provide recommendations, predictions or automated assessments, but the ultimate responsibility for corporate decisions remains connected with the human governance structure established under company law. The Companies Act therefore provides a foundation for arguing that directors must exercise appropriate supervision over AI systems used in material

[1] **The Companies Act, 2013**, § 166(1)–(2), Ministry of Corporate Affairs, Government of India, available at Ministry of Corporate Affairs — Companies Act, 2013 (accessed on 23 July 2026).

corporate functions.

Section 166(3) further requires directors to exercise their duties with due and reasonable care, skill and diligence and to exercise independent judgment.[2] These requirements acquire renewed importance where corporations rely upon algorithmic systems. A director who accepts an AI-generated recommendation without understanding its limitations, data sources, reliability or potential bias may face questions concerning the discharge of the statutory standard of care and independent judgment. AI should consequently be treated as an instrument supporting board decision-making rather than as a substitute for the legal judgment of directors. The increasing complexity of AI systems also makes technological literacy, appropriate internal controls and independent verification increasingly relevant aspects of responsible board governance.

The statutory architecture of corporate governance is supplemented, particularly for listed entities, by the Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015 ('SEBI LODR Regulations'). The regulatory framework imposes requirements concerning board composition, committees, risk management, disclosures and corporate governance reporting.[3] The importance of these requirements increases as AI becomes integrated into financial, operational and risk-management processes. In particular, the regulatory recognition of cybersecurity as a corporate governance concern demonstrates that technological risks are no longer merely technical matters but matters capable of affecting board-level accountability. SEBI's framework also requires disclosure of specified cybersecurity incidents, breaches or loss of data or documents as part of corporate governance compliance reporting.[4]

AI, Board Accountability, Data Protection and Cybersecurity

AI can substantially strengthen corporate governance by enabling continuous monitoring of corporate activities. AI-supported systems may identify suspicious transactions, unusual accounting patterns, potential insider risks, conflicts of interest and deviations from established compliance procedures. In this sense, AI can support audit committees, risk-management

[2] **Ibid.**, § 166(3)–(4). The provision requires directors to exercise due and reasonable care, skill and diligence and independent judgment.
[3] Securities and Exchange Board of India, **Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015**, Regulation 17–27, available at [SEBI — LODR Regulations, 2015]() (accessed on 23 July 2026).
[4] **Ibid.**, Regulation 27(2)(ba), concerning disclosure of specified cybersecurity incidents, breaches or loss of data or documents. (accessed on 24 July 2026).

committees and boards in fulfilling their oversight functions. AI can also facilitate predictive risk management by analysing historical and real-time information to identify emerging financial, operational and cybersecurity threats. However, these benefits must be balanced against the risks associated with algorithmic opacity, inaccurate data, discriminatory outputs, cybersecurity vulnerabilities and excessive dependence upon automated recommendations.

The Information Technology Act, 2000 provides an important component of India's legal framework for electronic governance and cybersecurity. Section 43A establishes liability in specified circumstances concerning failure by a body corporate to implement and maintain reasonable security practices and procedures in relation to sensitive personal data or information.[5] Although the regulatory landscape has evolved significantly following enactment of the Digital Personal Data Protection Act, 2023 ('DPDP Act'), the IT Act remains relevant to understanding corporate responsibilities in the digital environment. The Indian Computer Emergency Response Team (CERT-In), constituted under section 70B of the IT Act, also plays a central role in cybersecurity incident response. The CERT-In Directions of 28 April 2022 require covered entities to report specified cyber incidents within six hours of noticing them or becoming aware of them.[6] Such obligations demonstrate that cybersecurity governance can directly affect corporate compliance and therefore requires appropriate board oversight.

The Digital Personal Data Protection Act, 2023 introduces another important dimension to AI-based corporate governance. The Act seeks to regulate the processing of digital personal data while recognising the need for lawful processing and protection of individual data rights.[7] AI systems frequently depend upon large datasets, some of which may contain personal information relating to employees, customers, directors, shareholders or other stakeholders. Consequently, corporations deploying AI must consider whether their data collection, processing, storage and utilisation practices satisfy applicable data-protection requirements. The board therefore has an increasingly important responsibility to ensure that AI deployment is accompanied by appropriate data-governance mechanisms, security safeguards and organisational accountability.

[5] **The Information Technology Act, 2000**, § 43A, Ministry of Electronics and Information Technology, Government of India (accessed on 24 July 2026).
[6] Indian Computer Emergency Response Team, **Directions under Section 70B of the Information Technology Act, 2000**, 28 April 2022, available at CERT-In — Directions under Section 70B (accessed on 25 July 2026). CERT-In requires specified cyber incidents to be reported within six hours of noticing or becoming aware of them.
[7] **The Digital Personal Data Protection Act, 2023**, No. 22 of 2023, Ministry of Law and Justice, Government of India, available at Digital Personal Data Protection Act, 2023 (accessed on 25 July 2026).

The relationship between AI and board accountability becomes particularly significant where an AI system produces an erroneous or harmful recommendation. Existing Indian corporate law does not generally recognise AI as an independent bearer of fiduciary duties equivalent to those imposed upon directors. Therefore, responsibility cannot simply be transferred to the algorithm. Where an AI system is used to support a corporate decision, directors may need to demonstrate that reasonable procedures were followed in selecting, testing, monitoring and supervising the system. This may require documentation of the source and quality of data, validation of algorithms, assessment of cybersecurity risks, human review of significant AI-generated recommendations and periodic evaluation of system performance.

For listed companies, the connection between AI governance and disclosure is also becoming increasingly important. Corporate governance depends upon accurate and meaningful disclosure to shareholders and regulators. If AI is used in material financial, risk-management or compliance processes, inaccurate algorithmic outputs could potentially affect corporate disclosures and investor decision-making. The board must therefore ensure that reliance upon AI does not undermine the principles of accuracy, transparency and accountability that underpin securities regulation.[8]

Towards an AI-Enabled but Human-Accountable Corporate Governance Framework

The central legal challenge is therefore not whether corporations should use AI, but how AI can be incorporated without weakening established principles of human accountability. The Companies Act, 2013 places the legal responsibility for corporate governance upon directors and does not permit technological delegation to become a mechanism for avoiding fiduciary or statutory responsibilities. The board must consequently retain meaningful human oversight over material AI-assisted decisions. This principle is consistent with the broader corporate governance objective of ensuring that boards understand significant risks and establish appropriate internal control and monitoring mechanisms.[9]

[8] Securities and Exchange Board of India, **Format of Compliance Report on Corporate Governance by Listed Entities**, Circular No. SEBI/HO/CFD/CMD-2/P/CIR/2021/567, 31 May 2021, available at SEBI — Corporate Governance Compliance Report (accessed on 26 July 2026).

[9] Securities and Exchange Board of India, **Report of the Committee on Corporate Governance**, October 2017, discussing the role of the Risk Management Committee and the inclusion of cybersecurity within its functions, available at SEBI — Committee on Corporate Governance Report (accessed on 26 July 2026).

AI can enhance board accountability in at least four important ways. First, it can improve transparency by enabling systematic analysis of corporate information. Secondly, it can strengthen risk management through early identification of financial, operational and cyber risks. Thirdly, it can facilitate regulatory compliance by continuously monitoring applicable legal requirements and internal policies. Fourthly, AI can support audit and internal-control mechanisms by detecting anomalies and potentially fraudulent activities. Nevertheless, these benefits will only materialise where AI systems themselves are governed through clear accountability structures.

India therefore requires an integrated approach connecting corporate law, securities regulation, data protection and cybersecurity. Boards should establish AI governance policies identifying permissible uses of AI, responsibilities of directors and senior management, procedures for human review, data-protection safeguards, cybersecurity requirements and mechanisms for auditing algorithmic outcomes. Audit and risk-management committees should possess sufficient technological expertise to scrutinise AI-related risks. Companies should also maintain appropriate records demonstrating how material AI-supported decisions were reached, particularly where such decisions have implications for shareholders, employees, customers or regulatory compliance.

The future of Indian corporate governance is consequently likely to involve a model in which AI enhances—not replaces—human decision-making. The principal legal objective should be to ensure that technological efficiency operates alongside fiduciary responsibility, transparency and accountability. AI may substantially improve the capacity of boards to identify risks and make informed decisions, but the legal responsibility for corporate governance must remain attributable to identifiable human actors. A robust Indian framework should therefore combine technological innovation with board-level supervision, explainability, cybersecurity, data protection and effective regulatory oversight. Such an approach would enable corporations to benefit from AI while preserving the foundational principles of responsible corporate governance.

Research Objectives

1. To examine the role of Artificial Intelligence in strengthening corporate governance, transparency, risk management and decision-making in Indian companies.

2. To analyse the legal accountability of boards of directors for AI-assisted corporate decisions and identify regulatory measures for ensuring responsible and transparent AI governance in India.

Research methodology

The present study adopts a doctrinal and analytical research methodology to examine the role of Artificial Intelligence in enhancing corporate governance and board accountability in India. The research is primarily based on secondary sources, including statutory provisions, judicial decisions, regulatory guidelines, government reports, scholarly books, research articles, policy documents and authoritative online legal databases. Particular emphasis is placed on the Companies Act, 2013, Securities and Exchange Board of India regulations, Information Technology Act, 2000, Digital Personal Data Protection Act, 2023, and relevant cybersecurity and AI-related regulatory developments. The study analyses the statutory duties of directors, fiduciary obligations, corporate disclosure requirements, risk-management responsibilities and accountability arising from AI-assisted decision-making. A comparative approach is also adopted to examine relevant international developments, particularly the European Union and United States frameworks. The collected material is critically analysed to identify legal gaps, challenges relating to algorithmic transparency, data protection, cybersecurity and liability, and to formulate recommendations for strengthening responsible AI-based corporate governance in India.

Analysis

1. AI as an Instrument for Strengthening Corporate Governance and Decision-Making

The first objective of the study is to examine the role of Artificial Intelligence ('AI') in strengthening corporate governance, transparency, risk management and decision-making in Indian companies. The doctrinal analysis indicates that AI does not presently constitute an independent legal actor within Indian company law. Rather, it operates as a technological instrument through which directors, officers, auditors and compliance personnel may perform existing corporate functions more efficiently. This distinction is legally significant because the Companies Act, 2013 continues to place responsibility for corporate management and oversight upon human directors. Section 166 requires directors to act in good faith, promote the objects of the company, exercise due and reasonable care, skill and diligence, and exercise independent judgment.[10] Accordingly, the introduction of AI into boardrooms does not displace the fiduciary or statutory responsibilities of directors; instead, it potentially expands the range of information and analytical tools that directors must understand and supervise. The Act is therefore capable of accommodating AI-assisted governance, but it does not yet contain specific provisions dealing with algorithmic accountability, automated corporate decisions or AI-related board duties.

AI can improve corporate governance through automated analysis of financial statements, continuous monitoring of transactions, identification of unusual patterns, predictive risk assessment, compliance monitoring and cybersecurity surveillance. A board using AI-supported systems can potentially receive earlier warnings regarding fraud, liquidity problems, regulatory violations or cyber incidents. This can strengthen the effectiveness of internal controls and enable boards to move from predominantly reactive governance towards predictive risk management. The legal significance of such systems arises from the fact that the quality of board oversight increasingly depends upon the quality of information available to directors. AI can process large datasets beyond practical human capacity and consequently improve the informational foundation upon which directors exercise their judgment.

The development of regulatory technology within India's securities market provides an important illustration. SEBI has itself acknowledged the potential of AI-driven analytics in regulatory supervision. In a 2025 address, SEBI described its use of AI-driven analytics and predictive, rule-based alerts for identifying potentially manipulative trading patterns and stated that technological resilience must be treated as a boardroom priority.[11] This demonstrates that AI is not merely a future governance possibility; it is already being incorporated into regulatory surveillance. For corporate boards, the implication is that technological competence and oversight may increasingly become components of effective governance.

SEBI's Consultation Paper on Guidelines for Responsible Usage of AI/ML in Indian Securities Markets, issued on 20 June 2025, is particularly significant.[12] The consultation recognised the increasing use of AI/ML in securities-market activities and sought to establish principles for responsible usage. Its importance for corporate governance lies in its emphasis on

[10] **The Companies Act, 2013**, §§ 166(2)–(3), Ministry of Corporate Affairs, Government of India, available at Companies Act, 2013 (accessed on 23 July 2026).
[11] Securities and Exchange Board of India, **Address by the Chairman at the 25th ICSI National Awards for Excellence in Corporate Governance**, 19 December 2025, discussing AI-driven analytics, predictive surveillance and board-level technological resilience, available at SEBI Corporate Governance Address (accessed on 23 July 2026).
[12] Securities and Exchange Board of India, **Consultation Paper on Guidelines for Responsible Usage of AI/ML in Indian Securities Markets**, 20 June 2025, available at SEBI AI/ML Consultation Paper (accessed on 23 July 2026).

accountability, controls and responsible deployment rather than merely technological innovation. Although a consultation paper does not possess the same legal force as enacted legislation or binding regulations, it demonstrates the direction in which Indian securities regulation is moving. It supports the proposition that AI systems used by regulated entities should remain subject to identifiable human and institutional accountability.

The SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015 ('LODR Regulations') further reinforce this position. The current framework requires listed entities to maintain corporate governance structures and, importantly, provides for disclosure of specified cybersecurity incidents, breaches or loss of data or documents in the corporate-governance compliance report.[13] AI systems that control or assist financial reporting, investor communication, compliance monitoring or cybersecurity therefore have implications for disclosure and governance obligations. A material failure of an AI system could potentially become a corporate-governance issue where it affects the accuracy of disclosures, investor protection or risk management.

The 2024 SEBI proceedings concerning PTC India Financial Services Ltd. provide a useful Indian case study demonstrating that corporate governance failures are examined through the conduct and responsibilities of human decision-makers. SEBI investigated allegations arising from the resignations of independent directors and identified alleged breaches of corporate-governance requirements during the relevant examination period.[14] The matter is important for the present research because it reinforces a central principle: corporate governance obligations are institutional and board-centred. AI may assist directors in identifying governance risks, but the legal system continues to examine whether responsible human actors discharged their governance obligations. The lesson for AI-enabled companies is that algorithmic systems cannot be used as a shield against failures of board oversight.

2. AI, Directors' Duties and the Question of Accountability

The second objective is to analyse the legal accountability of boards of directors for AI-assisted corporate decisions. The doctrinal analysis demonstrates that the strongest existing legal basis for such accountability lies in section 166 of the Companies Act, 2013. The statutory

[13] Securities and Exchange Board of India, **SEBI (Listing Obligations and Disclosure Requirements) Regulations, 2015**, Regulation 27(2)(ba), current version amended up to January 2026, available at SEBI LODR Regulations (accessed on 24 July 2026).

[14] Securities and Exchange Board of India, **Order in the Matter of Corporate Governance Issues in PTC India Financial Services Ltd.**, WTM/ASB/CFD/CFD-SEC-2/30416/2024-25, 12 June 2024, available at SEBI PTC India Financial Services Order (accessed on 24 July 2026).

requirement of due and reasonable care, skill and diligence becomes particularly relevant when directors approve or rely upon AI systems. A director need not necessarily possess the technical ability to develop an AI model, but responsible governance increasingly requires directors to understand the material risks associated with systems on which important corporate decisions depend.

The requirement of independent judgment under section 166(3) is even more significant. If directors merely accept an AI-generated recommendation without questioning its assumptions, reliability, source data or potential biases, it could be argued that the board has allowed technology to replace rather than assist human judgment. AI-supported governance should consequently be based upon a principle of human accountability with technological assistance. For high-risk decisions—such as major acquisitions, related-party transactions, financial disclosures, employee termination systems, lending decisions or cybersecurity responses—boards should maintain mechanisms for human review and documented approval.

A recent decision of the Delhi High Court in ***Rajendra Sachdeva v. M/s A.C. Engineering Private Limited & Ors.*** (2025) is relevant to understanding the limits of personal liability of directors. The Court held, on the facts before it, that directors could not automatically be made personally liable for the company's contractual liability in the absence of a personal guarantee, indemnity or pleaded tortious conduct.[15] The decision reinforces the separate legal personality of the company and demonstrates that directors' personal liability cannot simply be presumed because they occupy the position of directors. At the same time, the judgment is useful for AI governance because it highlights the importance of identifying the precise legal basis upon which director liability is asserted. If an AI system causes corporate loss, the mere fact that a director sits on the board should not automatically establish personal liability. Liability would require examination of the director's actual role, statutory duties, knowledge, authorisation, negligence or other legally recognised basis.

This principle becomes especially important when AI systems are acquired from external vendors. A company may rely upon an AI provider for cybersecurity, recruitment, financial analysis or compliance. However, outsourcing technological functionality does not necessarily amount to outsourcing corporate responsibility. Boards must undertake appropriate due diligence regarding the vendor, algorithmic reliability, security architecture, data processing, contractual allocation of risk, audit rights and incident-response mechanisms.

[15] **Rajendra Sachdeva v. M/s A.C. Engineering Private Limited & Ors.**, RFA 633/2023, Delhi High Court, judgment dated 25 February 2025, available at Delhi High Court judgment (accessed on 24 July 2026).

The PTC India Financial Services proceedings further demonstrate the importance of board processes, independent directors and institutional controls.[16] In an AI environment, the same governance principles should extend to algorithmic decision-support systems. Audit committees, risk-management committees and independent directors should have access to sufficient technical information to challenge AI outputs where necessary. A governance framework in which directors receive unexplained algorithmic recommendations without adequate technical oversight would weaken rather than strengthen accountability.

The issue is also connected with data protection. The Digital Personal Data Protection Act, 2023 establishes obligations relating to the processing of digital personal data and imposes responsibilities upon data fiduciaries.[17] Corporate AI systems frequently process employee, customer, shareholder and other personal information. Therefore, AI governance cannot be separated from data governance. Boards should ensure that AI deployment incorporates lawful processing, appropriate safeguards, security measures and organisational accountability.

The Digital Personal Data Protection Rules, 2025 and the phased implementation framework further demonstrate that India's data-protection regime is becoming more operationally significant for corporations.[18] For companies using AI, this means that board-level governance must increasingly include data inventories, access controls, security safeguards, vendor management and mechanisms for responding to data incidents.

Cybersecurity presents an additional accountability dimension. CERT-In's directions under section 70B of the Information Technology Act, 2000 require covered entities to report specified cyber incidents within prescribed timelines.[19] AI systems themselves can become targets for prompt injection, data poisoning, model manipulation, unauthorised access and other forms of cyberattack. Thus, a board that adopts AI without assessing its cybersecurity vulnerabilities may create a new category of corporate risk. SEBI's cybersecurity and cyber-resilience framework for regulated entities, together with its subsequent clarifications and implementation extensions, demonstrates the movement towards treating cyber resilience as an institutional governance responsibility.[20]

---

[16] **PTC India Financial Services Ltd.**, supra note 5.

[17] **The Digital Personal Data Protection Act, 2023**, Ministry of Law and Justice, Government of India, available at Digital Personal Data Protection Act, 2023 (accessed on 25 July 2026).

[18] Ministry of Electronics and Information Technology, Government of India, **Digital Personal Data Protection Rules, 2025**, 14 November 2025, available at DPDP Rules 2025 (accessed on 25 July 2026).

[19] Indian Computer Emergency Response Team, **Directions under Section 70B of the Information Technology Act, 2000**, 28 April 2022, available at CERT-In Directions (accessed on 25 July 2026).

[20] Securities and Exchange Board of India, **Extension towards Adoption and Implementation of Cybersecurity and Cyber Resilience Framework (CSCRF) for SEBI Regulated Entities**, Circular No. SEBI/HO/ITD-1/ITD_CSC_EXT/P/CIR/2025/96, 30 June 2025, available at SEBI CSCRF Circular (accessed on 26 July 2026).

3. Case Studies and Emerging Legal Lessons

International case studies provide valuable evidence regarding the practical consequences of inadequate AI governance. The decision in ***Moffatt v. Air Canada***, 2024 BCCRT 149, is particularly instructive. Air Canada's website chatbot provided incorrect information concerning bereavement fares, and the customer relied upon that information. Air Canada argued, among other things, that the chatbot was a separate entity responsible for its own actions. The British Columbia Civil Resolution Tribunal rejected the attempt to avoid responsibility and found the airline liable in the circumstances.[21] Although the case arose in a consumer-law context rather than corporate law, its governance implication is substantial: a corporation cannot necessarily escape responsibility simply by attributing an erroneous corporate communication to an automated system. For Indian companies, the case provides a persuasive illustration of why AI outputs should be monitored, verified and subject to organisational controls.

A second important case study is the Amazon AI recruitment-system controversy. Amazon reportedly developed an experimental machine-learning system to evaluate job applicants, but the system was found to disadvantage women because the training data reflected historical patterns that favoured male applicants. Amazon ultimately abandoned the tool.[22] The case illustrates the governance problem of algorithmic bias. An AI system may appear technologically objective while reproducing historical discrimination contained in its training data. From an Indian corporate-governance perspective, boards deploying AI in recruitment, remuneration, credit assessment or customer profiling should therefore consider fairness, discrimination, explainability and auditability rather than treating algorithmic outputs as inherently neutral.

A third case study is the United States Securities and Exchange Commission's 2024 enforcement action against Delphia (USA) Inc. and Global Predictions Inc. Both investment advisers were charged with making false or misleading statements regarding their use of AI and agreed to pay a total of $400,000 in civil penalties.[23] The enforcement action is particularly relevant to corporate disclosure and investor protection. It establishes an important governance principle: companies should not exaggerate their AI capabilities merely because AI creates

---

[21] **Moffatt v. Air Canada**, 2024 BCCRT 149 (Civil Resolution Tribunal, British Columbia), discussed in Moffatt v. Air Canada analysis (accessed on 26 July 2026).

[22] Jeffrey Dastin, **Amazon Scraps Secret AI Recruiting Tool That Showed Bias Against Women**, Reuters, 10 October 2018, available at Reuters report on Amazon AI recruitment (accessed on 26 July 2026).

[23] U.S. Securities and Exchange Commission, **SEC Charges Two Investment Advisers with Making False and Misleading Statements About Their Use of Artificial Intelligence**, Press Release No. 2024-36, 18 March 2024, available at SEC AI-Washing Enforcement Release (accessed on 26 July 2026).

commercial or investment appeal. This phenomenon, commonly described as “AI washing,” demonstrates that AI-related corporate statements can generate regulatory consequences when they are inaccurate or misleading.

The lesson for Indian listed companies is directly relevant to disclosure obligations under securities regulation. If a company states that it employs sophisticated AI for fraud detection, investment analysis, cybersecurity or business forecasting, such representations should be accurate and capable of substantiation. Boards should therefore require appropriate verification of material AI-related claims before they are included in annual reports, investor presentations, public statements or regulatory disclosures.

The collective analysis of these case studies demonstrates that AI governance has at least five dimensions: accuracy, accountability, transparency, cybersecurity and human oversight. AI may enhance corporate governance by improving the speed and scale of analysis, but the same technology may amplify corporate risk when poorly governed. Consequently, the study finds that AI should be incorporated into the existing corporate-governance architecture rather than treated as an independent technological domain.

Discussion and Findings

The doctrinal analysis establishes that India's present framework provides a partial legal foundation for AI-enabled corporate governance but does not yet provide a comprehensive AI-specific regime for boards. Section 166 of the Companies Act can accommodate principles of human responsibility, care, skill and independent judgment, while SEBI's governance and cybersecurity framework provides additional obligations for listed entities. Data-protection and information-technology laws further regulate important components of AI deployment. However, there remains no comprehensive statutory framework expressly defining the board's responsibility for algorithmic governance, AI risk assessment, model validation, explainability or AI-related corporate disclosures.

The study therefore finds that AI should be treated as a board-level enterprise risk, particularly where it affects financial reporting, securities activities, personal data, cybersecurity, employment, consumer relations or strategic decision-making. Boards should establish AI governance policies, maintain an inventory of material AI systems, identify responsible executives, conduct periodic algorithmic risk assessments, require human review for high-impact decisions and maintain audit trails of significant AI-assisted decisions.

 ISSN: 2581-8503

The most appropriate regulatory model for India would not necessarily be a completely separate AI corporate statute. Instead, AI governance could initially be integrated into existing corporate, securities, cybersecurity and data-protection frameworks through sector-specific regulations and board-level governance requirements. SEBI's 2025 AI/ML consultation and its continuing cybersecurity framework illustrate how such sectoral regulation can develop incrementally.[24]

Ultimately, the research supports a "human-in-command" model of corporate AI governance. AI should enhance the board's capacity to analyse information and identify risks, but it should not become a mechanism through which directors avoid responsibility. The board must remain capable of explaining why an AI system was adopted, how its risks were assessed, what safeguards were implemented and how significant decisions were ultimately approved. Such an approach would allow Indian companies to obtain the efficiency benefits of AI while preserving the foundational corporate-law principles of fiduciary responsibility, transparency, independent judgment and accountability.

Conclusion

Artificial Intelligence is rapidly transforming the structure and functioning of corporate governance in India by enhancing decision-making, risk assessment, compliance monitoring, fraud detection, cybersecurity and corporate reporting. The analysis demonstrates that AI can significantly strengthen the capacity of boards of directors to process complex information and identify emerging corporate risks. However, technological efficiency cannot replace the fundamental principles of corporate accountability established under Indian corporate law. In particular, section 166 of the Companies Act, 2013 continues to impose duties of good faith, due care, skill, diligence and independent judgment upon directors, irrespective of whether corporate decisions are supported by AI systems.

The study further concludes that the increasing use of AI creates new dimensions of board responsibility. Directors must ensure appropriate human oversight, algorithmic reliability, data protection, cybersecurity, transparency and internal controls when adopting AI-based systems. Existing frameworks, including the Companies Act, 2013, SEBI regulations, the Information

[24] Securities and Exchange Board of India, **Consultation Paper on Guidelines for Responsible Usage of AI/ML in Indian Securities Markets**, supra note 3.

Technology Act, 2000, the Digital Personal Data Protection Act, 2023 and CERT-In requirements, provide important foundations, but they do not yet constitute a comprehensive framework specifically addressing AI-related corporate accountability.

Accordingly, India should adopt a human-centred AI governance model in which AI assists rather than replaces board judgment. Companies should develop AI governance policies, conduct periodic algorithmic and cybersecurity risk assessments, maintain audit trails and ensure meaningful human review of significant AI-assisted decisions. Ultimately, responsible integration of AI into corporate governance requires a balance between technological innovation and legal accountability. Strengthening this balance will promote transparency, investor confidence, corporate resilience and sustainable governance in India's increasingly digital corporate environment.

Suggestions

- **Develop AI Governance Policies:** Companies should adopt board-approved AI governance policies defining permissible uses, responsibilities, risk controls and accountability mechanisms.
- **Strengthen Board Expertise:** Directors should receive regular training on AI, cybersecurity, algorithmic risks, data protection and emerging technological regulations.
- **Ensure Human Oversight:** Significant AI-assisted corporate decisions should remain subject to meaningful human review and independent board judgment.
- **Conduct AI Risk Audits:** Companies should periodically evaluate AI systems for accuracy, bias, cybersecurity vulnerabilities, privacy risks and regulatory compliance.
- **Improve Transparency:** Material reliance on AI should be appropriately documented and disclosed to relevant stakeholders wherever legally or commercially necessary.
- **Strengthen Cybersecurity:** AI systems should be integrated with robust cybersecurity, incident-response and data-protection mechanisms.
- **Develop Clear Regulations:** Indian regulators should establish specific guidelines addressing AI accountability, algorithmic transparency, board responsibilities and corporate liability.

Future scope

Future research may examine sector-specific AI governance frameworks for Indian companies and develop measurable standards for algorithmic transparency, board oversight and AI-related liability. Comparative studies involving India, the European Union and the United States can further evaluate emerging regulatory approaches, cybersecurity risks and evolving directors' duties in AI-driven corporate governance.